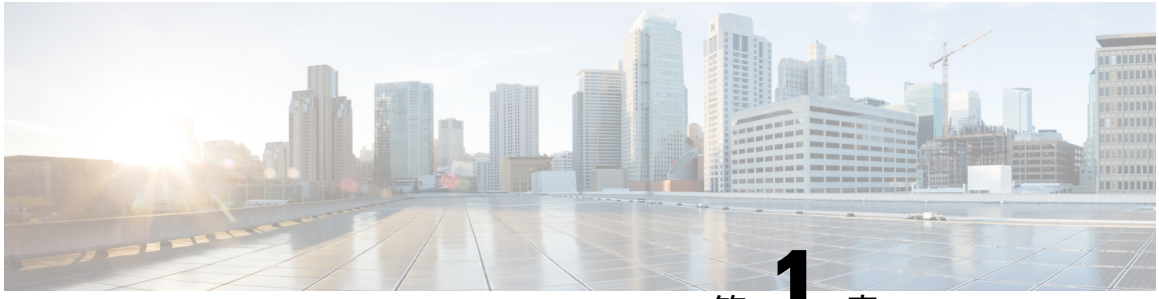
SD-Routing デバイスの設定グループ

最終更新：2025 年 7 月 8 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

設定グループの新機能または変更された機能

設定グループは、Cisco Catalyst SD-WAN Manager の設定にシンプルで再利用可能な構造化されたアプローチを提供します。設定グループは、SD-Routingデバイスをプロビジョニングするために使用されます。

次の表に、このドキュメントで説明する機能のリリースおよび関連情報を示します。これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

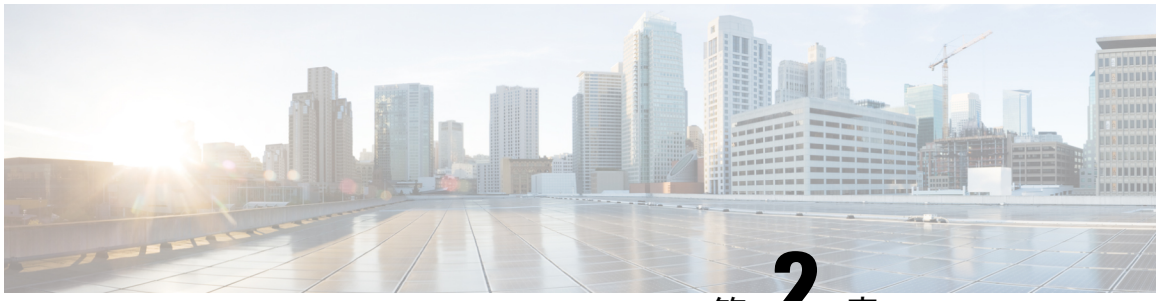
表 *1:* 機能の履歴

機能名	リリース情報	説明
設定グループと機能プロファイル（フェーズ II）	Cisco IOS XE 17.14.1a	設定グループ機能には、次の拡張機能が導入されています。 **Service Profile** • ACL IPv4 • IPv6 ACL • ルート ポリシー（ルート ポリシー） • VRF • オブジェクトトラッカー • オブジェクト トラッカー グループ • DHCP サーバー **トランスポートプロファイル** • トランスポート VPN • 管理 VPN • ACL IPv4 • IPv6 ACL • ルート ポリシー（ルート ポリシー） • VRF • オブジェクトトラッカー • オブジェクト トラッカー グループ

機能名	リリース情報	説明
設定グループと機能プロファイル（フェーズ I)	Cisco IOS XE 17.13.1a	このリリースでは、システムプロファイルで次の機能のサポートが導入されています。 • AAA • バナー • グローバル • ロギング • NTP • SNMP • フレキシブルポート速度 • CA Certificate
設定グループと機能プロファイル	Cisco IOS XE リリース 17.13.1a	設定グループおよび設定グループワークフロー機能が導入されました。

第 I 部

設定グループを使用したSD-Routingデバイスのプロビジョニング



第 2 章

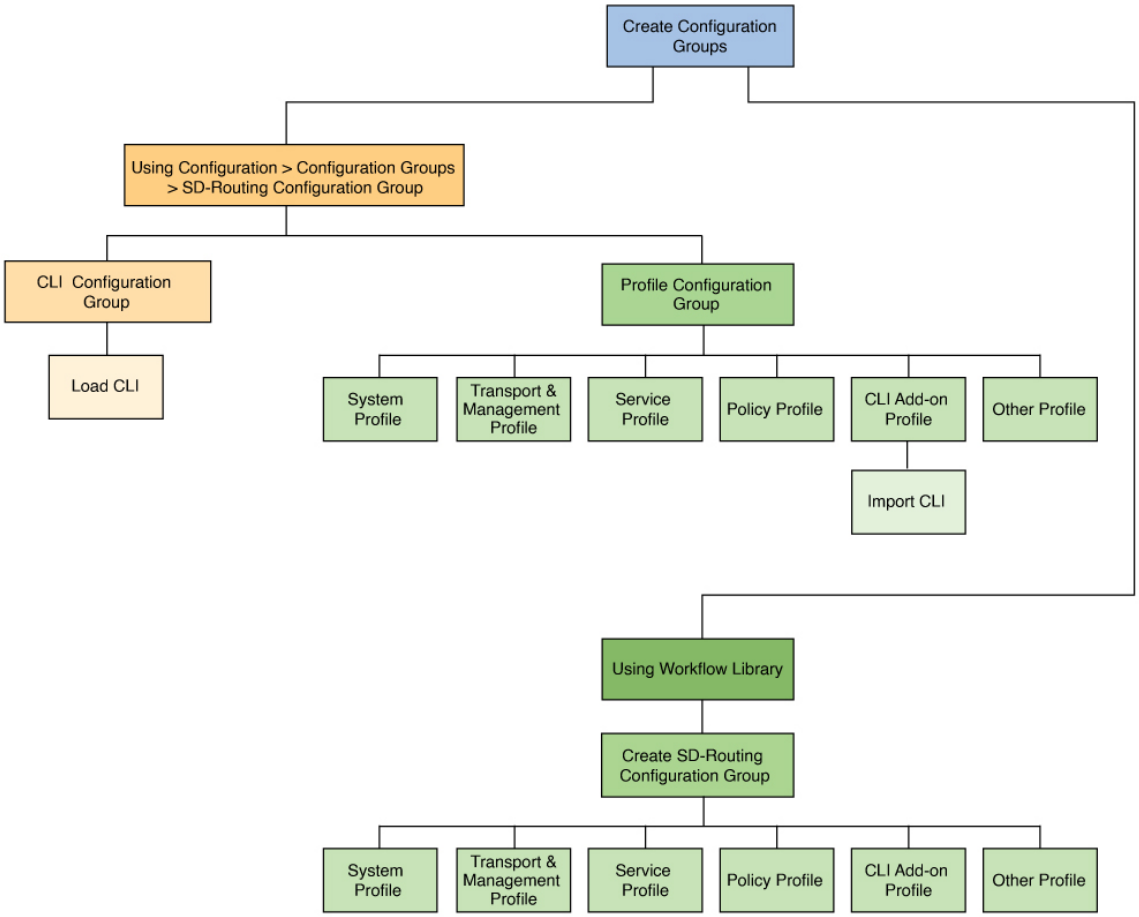
SD-Routing デバイスの設定グループについて

デバイスがオンボードされると、Cisco Catalyst SD-WAN Manager は該当する設定に基づいてデバイスをプロビジョニングします。設定グループを使用することで、このプロビジョニングプロセスが合理化されます。

Cisco SD-WAN Manager の設定グループは、デバイス固有の設定を作成して SD-Routing デバイスに適用するためのシンプルで再利用可能な構造化されたアプローチを提供します。設定グループは、機能プロファイル、機能、およびサブ機能で構成されます。

- 設定グループ：設定グループは機能または設定の論理グループであり、Cisco SD-WAN Manager によって管理されるネットワーク内の 1 つ以上のデバイスに適用できます。このグループ化は、ビジネスニーズに基づいて定義およびカスタマイズできます。
- 機能プロファイル：機能プロファイルは、さまざまな設定グループ間で再利用できる設定の柔軟な構成要素です。必要な機能、推奨される機能、または独自に使用される機能に基づいてプロファイルを作成し、プロファイルを組み合わせてデバイス設定を完成させることができます。
- 機能：機能プロファイルは機能で構成されます。機能は、さまざまな設定グループ間で共有する個々の機能です。

Cisco Catalyst SD-WAN Manager では、設定グループを作成する方法がいくつか用意されています。



1 [Configuration] メニューを使用した SD-Routing の設定グループの作成
2 CLI 設定グループを使用した設定グループの作成 （9 ページ）
3 プロファイル設定グループを使用した設定グループの作成 （10 ページ）
4 ワークフローライブラリを使用した SD-Routing の設定グループの作成 （12 ページ）

- 設定グループの前提条件 （9 ページ）
- 設定グループでサポートされるデバイス （9 ページ）
- [Configuration Group] メニューを使用した SD-Routing の設定グループの作成 （9 ページ）
- 設定グループと SD-Routing デバイスの関連付けおよび展開 （12 ページ）
- ワークフローライブラリを使用した SD-Routing の設定グループの作成 （12 ページ）
- [Deploy Configuration Group] ワークフローを使用した SD-Routing デバイスの展開 （13 ページ）

設定グループの前提条件

設定グループを使用するために必要な Cisco SD-Routing デバイスの最小ソフトウェアバージョンは、Cisco IOS XE リリース 17.13.1a です。

設定グループでサポートされるデバイス

設定グループのプロビジョニングは、次のプラットフォームでサポートされます。

- Cisco Catalyst 8000V シリーズ エッジ プラットフォーム、Cisco Catalyst 8200 シリーズ エッジプラットフォーム、Cisco Catalyst 8300 シリーズエッジプラットフォーム、Cisco Catalyst 8500 シリーズ エッジ プラットフォーム
- Cisco 1000 シリーズ サービス統合型ルータ。ただし、ISR1100-4G/6G および ISR1100X-4G/6G は SD-Routing モードをサポートしていません。
- Cisco Catalyst IR1100 高耐久性シリーズ ルータ

[Configuration Group] メニューを使用した SD-Routing の設定グループの作成

Cisco Catalyst SD-WAN Manager の [Configuration Group] メニューは、SD-Routing デバイスの設定を組み立てるための構成要素を提供します。推奨される方法は、既存のデバイスか新しいデバイスかによって異なります。

- 既存のデバイスの場合は、CLI 設定グループを使用して設定グループを作成します。
- 新しいデバイスの場合は、プロファイルベースの設定グループを使用して設定グループを作成します。

CLI 設定グループを使用した設定グループの作成

Cisco Catalyst SD-WAN Manager の [Configuration Groups] メニューから、SD-Routing デバイスの設定グループを簡単に作成できます。既存の SD-Routing デバイスを Cisco SD-WAN Manager にオンボードした後、**CLI 設定グループ**を使用してデバイスの実行コンフィギュレーションをロードし、設定を変更してから、これらのデバイスに展開します。

SD-Routing デバイスの CLI 設定グループを作成するには、説明されている手順を実行します。

始める前に

- オンボードしたデバイスが Cisco SD-WAN Manager で到達可能であることを確認してください。

- 展開に必要な設定を確実に理解しておいてください。

手順

ステップ 1 Cisco Catalyst SD-WAN Manager のメニューから**[Configuration]** > **[Configuration Groups]**の順に選択し、[Solution] で [SD-Routing] を選択します。

ステップ 2 [Create Configuration Group] をクリックします。

ステップ 3 名前と説明を追加し、[CLI Configuration Group] を選択してから [Create] をクリックします。

ステップ 4 [CLI]ペインで到達可能なデバイスを選択し、実行コンフィギュレーションをロードします。デバイス構成に YANG モデルが関連付けられていない場合は、その旨がプロンプトに示されます。

ヒント
デバイス構成は**[Configuration]** > **[WAN Edge List]**を選択するとデバイスの横に表示されます。デバイスを選択してから [Action] ボタンをクリックして、サポートされていない構成を確認します。

ステップ 5 [Yes] をクリックして実行コンフィギュレーションに保存します。

次のタスク

設定グループと SD-Routing デバイスの関連付けおよび展開 （12 ページ）

プロファイル設定グループを使用した設定グループの作成

Cisco Catalyst SD-WAN Manager の [Configuration Groups] メニューから、SD-Routing デバイスの設定グループを簡単に作成できます。構成要素（機能プロファイル、機能、サブ機能）をすばやく組み合わせて設定グループを作成し、それを展開して SD-Routing デバイスをプロビジョニングできます。

SD-Routingデバイスのプロファイルベースの設定グループを作成するには、説明されている手順を実行します。

始める前に

展開に必要な設定を確実に理解しておいてください。

手順

ステップ 1 Cisco Catalyst SD-WAN Manager のメニューから**[Configuration]** > **[Configuration Groups]**の順に選択し、[Solution] で [SD-Routing] を選択します。

ステップ 2 [Create Configuration Group] をクリックします。

ステップ 3 名前と説明を追加し、[Create] をクリックします。

ステップ 4 [System Profile]、[Transport&Management Profile]、[Service Profile] を作成し、これらのプロファイルに機能を追加します。機能とサブ機能の追加方法については、機能プロファイルへの機能とサブ機能の追加 （11 ページ）を参照してください。

ヒント
[Workflow Library] から、上記のプロファイルを使用して SD-Routing の設定グループを自動作成できます。ワークフローライブラリを使用した SD-Routing の設定グループの作成 （12 ページ）

ステップ 5 [CLI Add-on Profile] を作成して、他の設定グループ機能では使用できないデバイス設定を追加します。これらのコマンドを [CLI Configuration] エリアに追加するか、[Import Config File] をクリックして、設定をインポートして保存できます。

次のタスク

設定グループと SD-Routing デバイスの関連付けおよび展開 （12 ページ）

機能プロファイルへの機能とサブ機能の追加

始める前に

事前に設定グループを作成する必要があります。

手順

ステップ 1 Cisco Catalyst SD-WAN Manager で、SD-Routing の設定グループを選択し、[...] をクリックして編集します。
ステップ 2 機能プロファイルをクリックして開きます。
ステップ 3 [Add New Feature] をクリックして、ドロップダウンリストから機能を選択します。
ステップ 4 機能の名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
ステップ 5 機能の説明を入力します。説明は英数字とスペースのみを使用して、2048 文字以内で指定します。
ステップ 6 必要に応じてオプションを設定します。一部のパラメータには範囲のドロップダウンリストがあり、パラメータ値として [Global]、[Device Specific]、または [Default] を選択できます。表に記載されているようにプリファレンスを選択します。
ステップ 7 必要に応じてサブ機能を追加します。
ステップ 8 [Save] をクリックして、機能プロファイルに機能を追加します。

次のタスク

設定グループと SD-Routing デバイスの関連付けおよび展開 （12 ページ）

設定グループと SD-Routing デバイスの関連付けおよび展開

このタスクでは、設定グループの設定の確認、デバイスと設定グループの関連付け、および 1 つ以上の SD-Routing デバイスのプロビジョニングを行います。

始める前に

選択した設定グループが SD-Routing の設定グループであることを確認します。

手順

ステップ 1 Cisco SD-WAN Manager で、前に作成した**設定グループ**を選択します。

ステップ 2 [+Add] をクリックして、リストからデバイスを確認します。[Save] をクリックして、選択したデバイスに設定グループを割り当てます。

ステップ 3 設定変更をプロビジョニングするには、[Deploy] をクリックします。

ステップ 4 設定変更をプロビジョニングするデバイスを選択します。[Next] をクリックします。

ステップ 5 デバイスごとに、設定に基づいて変数を確認または更新します。[Next] をクリックします。

ステップ 6 デバイス設定の変更内容を確認する場合は、[Preview CLI] をクリックします。

デバイス設定が正しくない場合、画面の左上にエラーメッセージが表示され、問題が強調表示されます。

a) 設定グループに戻り、無効な設定を特定して修正します。
b) [Deploy Configuration Group] ワークフローで [Deploy] をクリックしてデバイスの設定変更をプロビジョニングして、変更を再度確認します。
c) デバイスを選択して、[CLI] ペインで設定変更を縦並びまたは横並びで表示します。削除された設定は赤色で強調表示され、新しい設定は緑色で強調表示されます。
d) 戻って展開を続行します。

ステップ 7 展開ステータスを表示して、ログでデバイスのプロビジョニング完了が示されていることを確認します。

ワークフローライブラリを使用した SD-Routing の設定グループの作成

[Workflow Library] に表示される [Create SD Routing Config] ワークフローは、SD-Routing デバイスの設定グループを作成する際の流れを示す簡素化されたワークフローです。これは、設定グループをすばやく作成するための代替手段です。

始める前に

手順

ステップ 1 Cisco SD-WAN Manager のメニューから**[Workflows]** > **[Workflow Library]** > **[Create SD-Routing Config]**の順に選択します。

ステップ 2 名前と任意で説明を入力し、クリックして SD-Routing の設定グループを作成します。

ステップ 3 設定グループを選択し、必要なプロファイルを追加します。詳細については、プロファイル設定グループを使用した設定グループの作成 （10 ページ）を参照してください。

次のタスク

設定グループと SD-Routing デバイスの関連付けおよび展開 （12 ページ）

[Deploy Configuration Group] ワークフローを使用した SD-Routing デバイスの展開

始める前に

SD-Routing の設定グループを作成し、1 つまたは複数のデバイスを設定グループに関連付けておく必要があります。

手順

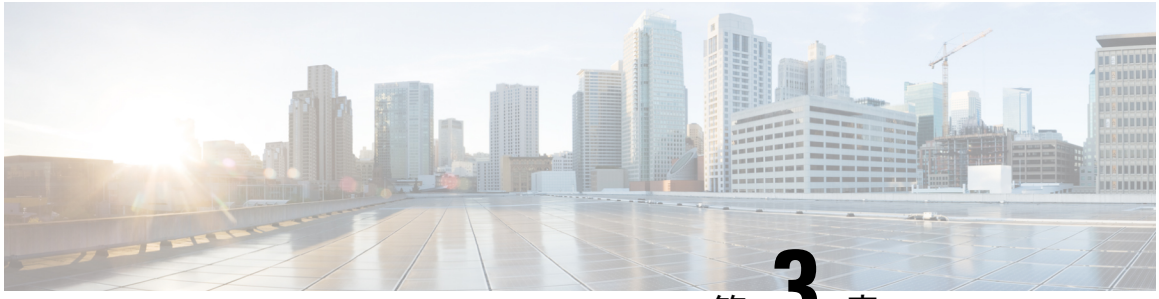
ステップ 1 Cisco SD-WAN Manager のメニューから**[Workflows]** > **[Workflow Library]**の順に選択します。

ステップ 2 [Deploy Configuration Group] ワークフローを開始します。

ステップ 3 ワークフローの指示に従ってください。

第 II 部

プロファイルベースの設定グループの構成要素



第 3 章

システム プロファイル

AAA

認証、許可、およびアカウンティング（AAA）機能は、Cisco SD-Routing デバイスにログインしているユーザーの認証、ユーザーに与える権限の決定、およびアクションのアカウンティングの実行をサポートします。

次の表では、AAA 機能を設定するためのオプションについて説明します。

ローカル

フィールド	説明
Add AAA User	
Name	ユーザーの名前を入力します。ユーザー名の長さは 1 ー 128 文字で、先頭は英字にする必要があります。名前に使用できるのは、英小文字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。英大文字は使用できません。 次のユーザー名は予約されているため、設定できません。backup、basic、bin、daemon、games、gnats、irc、list、lp、mail、man、news、nobody、proxy、quagga、root、sshd、sync、sys、uucp、および www-data。また、viptela-reserved で始まる名前は予約されています。

フィールド	説明
Password	ユーザーのパスワードを入力します。パスワードは MD5 ダイジェスト文字列で、タブ、復帰、改行などの任意の文字を含めることができます。詳細については、RFC 7950「The YANG 1.1 Data Modeling Language」のセクション 9.4 を参照してください。 各ユーザー名にはパスワードが必要です。ユーザーは自分のパスワードを変更できます。 管理ユーザーのデフォルトパスワードは admin です。このパスワードから変更することを強く推奨します。
Confirm Password	ユーザーのパスワードをもう一度入力します。
Privilege	特権レベル 1 または 15 から選択します。 • [Level 1]：ユーザー EXEC モード。読み取り専用です。アクセスできるコマンドは ping などに限定されています。 • [Level 15]：特権 EXEC モード。reload コマンドなど、すべてのコマンドにアクセスできます。また設定の変更も可能です。デフォルトで、特権レベル 15 の EXEC コマンドは、特権レベル 1 で使用できるコマンドのスーパーセットです。
公開キーチェーンの追加	
SSH RSA Key	[ssh-rsa] を選択します。

RADIUS

フィールド	説明
Add Radius Server	
IP Address (v4 or v6)	RADIUS サーバーホストの IP アドレスを入力します。
Acct Port	802.1X および 802.11i アカウンティング情報を RADIUS サーバーに送信するために使用する UDP ポートを入力します。 範囲：0 ～ 65535。 デフォルト：1813
Auth Port	RADIUS サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。 デフォルト：1812

フィールド	説明
Retransmit	デバイスが RADIUS 要求をサーバーに再送信する回数を入力します。 デフォルト：3 秒
Timeout	要求を再送信する前に、デバイスが RADIUS 要求への応答を待機する秒数を入力します。 デフォルト：5 秒 範囲：1 ～ 1000
Key*	認証と暗号化のために、Cisco SD-Routing デバイスから RADIUS サーバーに渡されるキーを入力します。
Key Type	[Protected Access Credential (PAC)] またはキータイプを選択します。

TACACS サーバー

フィールド	説明
Add TACACS Server	
IP Address (v4 or v6)	TACACS+ サーバーホストの IP アドレスを入力します。
Authentication Port	TACACS+ サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。 デフォルト：49
Timeout [second]	デバイスが TACACS+ 要求への応答を待機してから、要求を再送信する秒数を入力します。 デフォルト：5 秒 範囲：1 ～ 1000
Key	認証と暗号化のために、Cisco SD-Routing デバイスから TACACS+ サーバーに渡されるキーを入力します。キーを長さ 1 ～ 31 文字のテキスト文字列として入力すると、すぐに暗号化されます。または、AES 128 ビット暗号化キーを入力することもできます。キーは、TACACS+ サーバーで使用する AES 暗号化キーと一致させる必要があります。

アカウンティング

フィールド	説明
アカウンティングルールの追加	
Rule Id	アカウンティングルール ID を入力します。

フィールド	説明
Method	アカウンティング方式リストを指定します。次のいずれかを選択します。 • [commands]：特定の特権レベルに関連付けられた特定の個々の EXEC コマンドに関するアカウンティング情報を提供します。 • [exec]：ネットワーク アクセス サーバーでユーザー名、日付、開始および終了時間などのユーザー EXEC ターミナルセッションに関するアカウンティングレコードを提供します。 • [network]：ネットワークに関連するあらゆるサービス要求にアカウンティングを実行します。 • [system]：ユーザーに関連付けられていないすべてのシステムレベルのイベント（リロードなど）に対してアカウンティングを実行します。 （注） システムアカウンティングを使用しており、システムのスタートアップ時にアカウンティングサーバが到達不能である場合、システムに約2分間アクセスできません。
Start Stop	イベントの開始時にアカウンティング開始通知を送信し、イベントの終了時にレコード停止通知を送信する場合は、このオプションを有効にします。
Groups	以前に設定した TACACS グループを選択します。このアカウンティングルールが定義するパラメータは、このグループに関連付けられている TACACS サーバーによって使用されます。

許可

フィールド	説明
Console	コンソールアクセスコマンドの認証を実行するには、このオプションを有効にします。
Config Commands	コンフィギュレーションコマンドの認証を実行するには、このオプションを有効にします。
認証ルールの追加	
Rule Id	認証ルール ID を入力します。
Method	[Commands] を選択します。これにより、ユーザーが入力するコマンドが許可されます。
Level	許可するコマンドの権限レベル（1 または 15）を選択します。この権限レベルを持つユーザーが入力したコマンドが許可されます。

フィールド	説明
Authenticated	認証されたユーザーにのみ認証ルールパラメータを適用するには、このオプションを有効にします。このオプションを有効にしない場合、ルールはすべてのユーザーに適用されます。
Group(s)	以前に設定したTACACSグループを選択します。この認証ルールが定義するパラメータは、このグループに関連付けられているTACACSサーバーによって使用されます。

802.1X

フィールド	説明
Authentication Param	認証パラメータを有効にします。
Accounting Param	アカウンティングパラメータを有効にします。

認証と承認の順序

フィールド	説明
Server Auth Order	[local] を選択します。

バナー

バナー機能は、システムログインバナーの設定に役立ちます。

この機能のデフォルト値を持つ各パラメータでは、範囲が[Default]に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある[Scope]ドロップダウンをクリックし、次のいずれかを選択します。

次の表では、バナー機能を設定するためのオプションについて説明します。

フィールド	説明
Name	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
Login	ログインプロンプトの前に表示するテキストを入力します。ストリングの長さは、最大2048文字まで可能です。改行を挿入するには、\n と入力します。

フィールド	説明
Message of the Day	ログインバナーの前に表示する今日のメッセージのテキストを入力します。ストリングの長さは、最大 2048 文字まで可能です。改行を挿入するには、\n と入力します。

グローバル

グローバル機能は、HTTP、HTTPS、Telnet、IP ドメインルックアップ、およびその他のいくつかのデバイス設定など、デバイス上のさまざまなサービスを有効または無効にするのに役立ちます。

次の表では、グローバル機能を構成するためのオプションについて説明します。

サービス

フィールド	説明
HTTP Server	HTTP サーバーを有効または無効にします。
HTTPS Server	セキュア HTTPS サーバーを有効または無効にします。
FTP Passive	パッシブ FTP を有効または無効にします。
Domain Lookup	ドメインネームシステム（DNS）ルックアップを有効または無効にします。
ARP Proxy	プロキシ ARP を有効または無効にします。
RSH/RCP	デバイスでリモートシェル（RSH）とリモートコピー（rcp）を有効または無効にします。
Line Virtual Teletype (Configure Outbound Telnet)	アウトバウンド Telnet を有効または無効にします。
Cisco Discovery Protocol（CDP）	Cisco Discovery Protocol（CDP）を有効または無効にします。
Link Layer Discovery Protocol (LLDP)	リンク層検出プロトコル（LLDP）を有効または無効にします。
HTTP Client Source Interface	すべての HTTPS クライアント接続に送信元インターフェイスのアドレスを入力します。

NAT

フィールド	説明
NAT 64 UDP Timeout	UDP の NAT64 変換タイムアウトを指定します。 範囲：1 ～ 536870（秒） デフォルト：300 秒（5 分）
NAT 64 TCP Timeout	TCP の NAT64 変換タイムアウトを指定します。 範囲：1 ～ 536870（秒） デフォルト：3600 秒（1 時間）
NAT TCP Timeout	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：3600 秒（1 時間）
NAT 64 UDP Timeout	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：300 秒（5 分）

認証

フィールド	説明
HTTP Authentication	HTTP認証モードを選択します。 許容値：Local、AAA デフォルト：Local

SSH Version

フィールド	説明
SSH Version	SSHバージョンを選択します。 デフォルト：無効

Other Settings

フィールド	説明
TCP Keepalives (In)	着信ネットワーク接続がアイドル状態のときのキープアライブタイマーの生成を有効または無効にします。
TCP Keepalives (Out)	発信ネットワーク接続がアイドル状態のときのキープアライブタイマーの生成を有効または無効にします。
TCP Small Servers	小規模な TCP サーバー（ECHO など）を有効または無効にします。
UDP Small Servers	小規模な UDP サーバー（ECHO など）を有効または無効にします。
Console Logging	コンソールロギングを有効または無効にします。デフォルトでは、ルータはすべてのログメッセージをコンソールポートに送信します。
IP Source Routing	IP ソースルーティングを有効または無効にします。IP ソースルーティングは、パケットの発信元が、パケットが宛先に到達するために使用するパスを指定できるようにする機能です。
VTY Line Logging	デバイスがログメッセージをリアルタイムで vty セッションに表示することを有効または無効にします。
SNMP IFINDEX Persist	デバイスの再起動時に保持および使用されるインターフェイス インデックス（ifIndex）値を提供する SNMP IINDEX パーシステンスを有効または無効にします。
Ignore BOOTP	BOOTP サーバーを有効または無効にします。有効にすると、デバイスは 0.0.0.0 から送信される BOOTP パケットをリッスンします。無効にすると、デバイスはこれらのパケットを無視します。

ロギング

ロギング機能は、ローカルハードドライブまたはリモートホストへのロギングを構成するのに役立ちます。

次の表では、ロギング機能を設定するためのオプションについて説明します。

フィールド	説明
Max File Size(In Megabytes)	syslog ファイルの最大サイズを入力します。syslog ファイルは、ファイルサイズに基づいて 1 時間ごとにローテーションされます。ファイルサイズが設定値を超えると、ファイルがローテーションされ、syslog プロセスに通知されます。 範囲：1 ～ 20 MB デフォルト：10 MB

フィールド	説明
Rotations	最も古いファイルを破棄するまでに作成できる syslog ファイルの数を入力します。 範囲：1 ～ 10 デフォルト：10

TLS プロファイル

フィールド	説明
Add TLS Profile	
TLS Profile Name	TLS プロファイル名を入力します。
TLS Version	TLS バージョンを選択します。 • TLSv1.1 • TLSv1.2
Authentication Type*	サーバーを選択します。

フィールド	説明
Cipher Suite List	TLS バージョンに基づいて、暗号スイート（暗号化アルゴリズム）のグループを選択します。 暗号スイートのリストを以下に示します。 • [aes-128-cbc-sha]：暗号化タイプ tls_rsa_with_aes_cbc_128_sha • [aes-256-cbc-sha]：暗号化タイプ tls_rsa_with_aes_cbc_256_sha • [dhe-aes-cbc-sha2]：暗号化タイプ tls_dhe_rsa_with_aes_cbc_sha2（TLS1.2 以上） • [dhe-aes-gcm-sha2]：暗号化タイプ tls_dhe_rsa_with_aes_gcm_sha2（TLS1.2 以上） • [ecdhe-ecdsa-aes-gcm-sha2]：暗号化タイプ tls_ecdhe_ecdsa_aes_gcm_sha2（TLS1.2 以上）SuiteB • [ecdhe-rsa-aes-cbc-sha2]：暗号化タイプ tls_ecdhe_rsa_aes_cbc_sha2（TLS1.2 以上） • [ecdhe-rsa-aes-gcm-sha2]：暗号化タイプ tls_ecdhe_rsa_aes_gcm_sha2（TLS1.2 以上） • [rsa-aes-cbc-sha2]：暗号化タイプ tls_rsa_with_aes_cbc_sha2（TLS1.2 以上） • [rsa-aes-gcm-sha2]：暗号化タイプ tls_rsa_with_aes_gcm_sha2（TLS1.2 以上）

サーバ

フィールド	説明
サーバの追加	
IPv4 Address	syslog メッセージを保存するシステムの DNS 名、ホスト名、または IP アドレスを入力します。 別の syslog サーバーを追加するには、プラス記号（+）をクリックします。syslog サーバーを削除するには、エントリの右側にあるごみ箱のアイコンをクリックします。
VRF	syslog サーバーが配置されている VPN の識別子、または syslog サーバーに到達できる VPN の識別子を入力します。 範囲：0 ～ 65530

フィールド	説明
Source Interface	発信システムログメッセージに使用する特定のインターフェイスを入力します。このインターフェイスは、syslog サーバーと同じ VPN 内にある必要があります。それ以外の場合、設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスは syslog サーバーすべてで同じにする必要があります。
Severity	保存する syslog メッセージの重大度を選択します。重大度は、メッセージを生成したイベントの重大度を示します。優先順位は次のいずれかです。 • [informational]：ルーチンの状態（デフォルト）（syslog 重大度 6 に対応） • [debugging]：問題のデバッグに役立つ追加のログを出力します。 • [notice]：正常だが重大な状態（syslog 重大度 5 に対応） • [warn]：軽微なエラー状態（syslog 重大度 4 に対応） • [error]：システムの利便性を完全に損なわないエラー状態（syslog 重大度 3 に対応） • [critical]：重大な状態（syslog 重大度 2 に対応） • [alert]：すぐにアクションを実行する必要があります（syslog の重大度 1 に対応） • [emergency]：システムは使用できません（syslog 重大度 0 に対応）
TLS Enable	このオプションを有効にすると、TLS を介した syslog が許可されます。このオプションを有効にすると、次のフィールドが表示されます。 [TLS Properties Custom Profile]：TLS プロファイルを選択するには、このオプションを有効にします。このオプションを有効にすると、次のフィールドが表示されます。 [TLS Properties Profile]：IPv4 サーバー構成でサーバーまたは相互認証用に作成した TLS プロファイルを選択します。
IPv6 サーバーの追加	
IPv6 Address*	syslog メッセージを保存するシステムの DNS 名、ホスト名、または IP アドレスを入力します。 別の syslog サーバーを追加するには、プラス記号（+）をクリックします。syslog サーバーを削除するには、エントリの右側にあるごみ箱のアイコンをクリックします。

フィールド	説明
VRF	syslog サーバーが配置されている VPN の識別子、または syslog サーバーに到達できる VPN の識別子を入力します。 範囲：0 ～ 65530
Source Interface	発信システムログメッセージに使用する特定のインターフェイスを入力します。このインターフェイスは、syslog サーバーと同じ VPN 内にある必要があります。それ以外の場合、設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスは syslog サーバーすべてで同じにする必要があります。
Priority	保存する syslog メッセージの重大度を選択します。重大度は、メッセージを生成したイベントの重大度を示します。優先順位は次のいずれかです。 • [informational]：ルーチンの状態（デフォルト）（syslog 重大度 6 に対応） • [debugging]：問題のデバッグに役立つ追加のログを出力します。 • [notice]：正常だが重大な状態（syslog 重大度 5 に対応） • [warn]：軽微なエラー状態（syslog 重大度 4 に対応） • [error]：システムの利便性を完全に損なわないエラー状態（syslog 重大度 3 に対応） • [critical]：重大な状態（syslog 重大度 2 に対応） • [alert]：すぐにアクションを実行する必要があります（syslog の重大度 1 に対応） • [emergency]：システムは使用できません（syslog 重大度 0 に対応）
TLS Enable	このオプションを有効にすると、TLS を介した syslog が許可されます。
TLS Properties Custom Profile*	TLS プロファイルを選択するには、このオプションを有効にします。
TLS Properties Profile	IPv6 サーバー構成でサーバーまたは相互認証用に作成した TLS プロファイルを選択します。

NTP

Network Time Protocol（NTP）は、サーバーとクライアントの分散ネットワークがネットワーク全体で時刻を同期できるようにするプロトコルです。NTP 機能は、Cisco SD-WAN ネットワークで NTP 設定を行うのに役立ちます。

次の表では、NTP 機能を設定するためのオプションについて説明します。

サーバ

フィールド	説明
サーバの追加	
Hostname/IP address	NTP サーバーの IP アドレスか、NTP サーバーへの到達方法を認識している DNS サーバーの IP アドレスを入力します。
VRF to reach NTP Server*	NTP サーバーに到達するために使用する VRF 名を入力します。32 文字以内の英数字で指定します
Set authentication key for the server	MD5 認証を有効にするために、NTP サーバーに関連付けられた MD5 キーを指定します。 キーを有効にするには、[Authentication] の [Trusted Key] フィールドでキーを「trusted」とマークする必要があります。
Set NTP version	NTP プロトコルソフトウェアのバージョン番号を入力します。 範囲：1 ～ 4 デフォルト：4
Set interface to use to reach NTP server	NTP パケットの発信に使用する特定のインターフェイスの名前を入力します。このインターフェイスは、NTP サーバーと同じ VPN 内にある必要があります。そうでない場合、設定は無視されます。
Prefer this NTP server*	複数の NTP サーバーが同じストラタムレベルにあり、そのうちの 1 つを優先する場合は、このオプションを有効にします。別のストラタムレベルのサーバーについては、Cisco SD-Routing は最上位のストラタムレベルのサーバーを選択します。

認証

フィールド	説明
認証キーの追加	
Key Id	MD5 認証キー ID を入力します。 範囲：1 ～ 65535
MD5 Value*	MD5 認証キーを入力します。クリアテキストキーまたは AES 暗号化キーを入力します。

Advanced

フィールド	説明
Authoritative NTP Server	サポートされている 1 つまたは複数のルータをプライマリ NTP ルータとして設定する場合は、ドロップダウンリストから [Global] を選択し、このオプションを有効にします。 このオプションを有効にすると、次のフィールドが表示されます。 **Stratum**：プライマリ NTP ルータのストラタム値を入力します。ストラタム値は、基準クロックからのルータの階層的距離を定義します。 有効な範囲：1 ～ 15 の整数。値を入力しない場合、システムはルータの内部クロックのデフォルトストラタム値である 8 を使用します。
Source	NTP 通信の出口インターフェイスの名前を入力します。設定されている場合、システムは NTP トラフィックをこのインターフェイスに送信します。 たとえば、**GigabitEthernet1** または **Loopback0** と入力します。

SNMP

アプリケーション層の簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の対話用の通信標準規格を提供します。このプロトコルは、ネットワークデバイスのモニタリングや管理に共通して使用される標準化された言語を定義します。SNMP 機能は、Cisco SD-Routing デバイスで SNMP 機能を設定するのに役立ちます。

次の表では、SNMP 機能を設定するためのオプションについて説明します。

SNMP

表 2 : Advanced

フィールド	説明
Shutdown	デフォルトでは、SNMP は有効になっています。
Contact Person	Cisco SD-Routing デバイスの管理を担当するネットワーク管理担当者の名前を入力します。これには、最大 255 文字を使用できます。
Location of Device	デバイスのロケーションの説明を入力します。これには、最大 255 文字を使用できます。

SNMP バージョン

表 *3 :* 基本 *(Basic)*

フィールド	説明
SNMP バージョン（SNMP Version）	次の SNMP バージョンのいずれかを選択します。 • SNMP v2 • **SNMP v3**
SNMP v2：ビューの追加	
Name	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。コミュニティを追加する前にすべてのビューにビュー名を追加する必要があります。
Add OID	このオプションをクリックして、オブジェクト識別子（OID）を追加し、次のパラメータを構成します。 • [Id]：オブジェクトの OID を入力します。たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 を入力します。Cisco SD-Routing デバイス MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 を入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 • [Exclude]：このオプションを有効にして OID をビューに含めるか、このオプションを無効にして OID をビューから除外します。

フレキシブルポート速度

フレキシブルポート速度機能は、Cisco Catalyst 8500-12X4QC ルータにのみ適用されます。この機能を使用して、要件に基づいて 100GE、40GE、10GE、または 1GE として動作するようにインターフェイスを設定します。ポートタイプに対して行った変更は、設定グループをデバイスに適用した後にのみ有効になります。

フレキシブルポート速度機能を使用してポート設定を更新すると、一部のポートが有効になり、他のポートが無効になる場合があります。たとえば、デフォルトでは C8500-12X4QC はベイ 1 を 10GE モードで、ベイ 2 を 40GE モードで動作させます。ベイ 1 のモードは、10GE、40GE、または 100GE にできます。ベイ 1 を 100GE に設定すると、ベイ 0 のすべてのポートが無効になります。詳細については、Cisco Catalyst 8500-12X4QC デバイスガイドの「Bay Configuration」[英語] を参照してください。

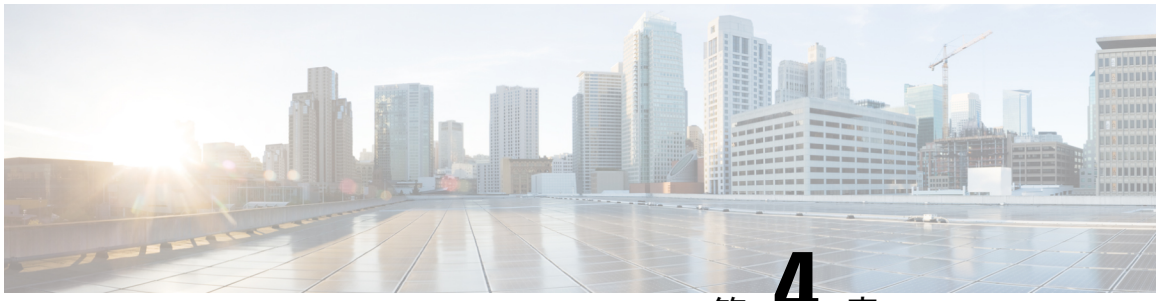
Cisco Catalyst 8500-12X4QC プラットフォームの各ベイのポートオプションの詳細については、『*Cisco Catalyst 8500 Series Edge Platforms Data Sheet*』の C8500-12X4QC 製品概要を参照してください。

一部のパラメータには範囲のドロップダウンリストがあり、パラメータ値として [Global]、[Device Specific]、または [Default] を選択できます。以下に示す表の説明に従って、次のオプションのいずれかを選択します。

パラメータの範囲	範囲の説明
グローバル（地球のアイコン）	パラメータの値を入力し、その値をすべてのデバイスに適用します。 デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU などがあります。
デバイス固有（ホストのアイコン）	デバイス固有の値がパラメータに使用されます。 [Device Specific] を選択すると、フィールドにキーの値を入力できます。キーは、パラメータの識別に役立つ一意の文字列です。デフォルトのキー値を変更するには、フィールドに新しい文字列を入力します。 デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID などがあります。
デフォルト（チェックマークで示されます）	デフォルト設定を持つパラメータには、デフォルト値が表示されます。

基本設定

パラメータ名	説明
Port Type	次のポートの組み合わせのいずれかを選択します。 • 12 ports of 1/10GE + 3 ports of 40GE • 8 ports of 1/10GE + 4 ports of 40GE • 2 ports of 100GE • 12 ports of 1/10GE + 1 port of 100GE • 8 ports of 1/10GE + 1 port of 40GE + 1 port of 100GE • 3 ports of 40GE + 1 port of 100GE デフォルトは、[12 ports of 1/10GE + 3 ports of 40GE] です。



第 4 章

トランスポートおよび管理のプロファイル

トランスポートおよび管理プロファイルは、WAN レベルで VRF を設定するのに役立ちます。この機能のデフォルト値を持つ各パラメータでは、範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。

トランスポート VRF

トランスポート VPN 機能は、WAN で VRF を設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。

次の表では、トランスポート VPN 機能を設定するためのオプションについて説明します。

基本設定

フィールド	説明
VRF	VRF の ID を入力します。
Enhance ECMP Keying	ECMP ハッシュキーとして、送信元 IP アドレス、宛先 IP アドレス、プロトコル、および DSCP フィールドの組み合わせの使用に加えて、レイヤ 4 の送信元ポートと宛先ポートの ECMP ハッシュキーでの使用を有効にします。 デフォルト：無効

DNS

フィールド	説明
Add DNS	
Primary DNS Address (IPv4)	この VRF のプライマリ IPv4 DNS サーバーの IP アドレスを入力します。
Secondary DNS Address (IPv4)	この VRF のセカンダリ IPv4 DNS サーバーの IP アドレスを入力します。
DNS IPv6 を追加	
Primary DNS Address (IPv6)	この VRF のプライマリ IPv6 DNS サーバーの IP アドレスを入力します。
Secondary DNS Address (IPv6)	この VRF のセカンダリ IPv6 DNS サーバーの IP アドレスを入力します。

ホストマッピング

フィールド	説明
新規ホストマッピングの追加	
Hostname	DNS サーバーのホスト名を入力します。名前には最大 128 文字を使用できます。
List of IP	ホスト名に関連付ける IP アドレスを 14 個まで入力します。エントリをカンマで区切ります。

ルート

フィールド	説明
IPv4スタティックルートの追加	
Network address	IPv4 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VRF で構成する IPv4 スタティック ルートのプレフィックス長を入力します。
Subnet Mask*	サブネット マスクを入力します。

フィールド	説明
Gateway*	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [nextHop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]：ネクストホップ IPv4 アドレスを入力します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • **[dhcp]** • [null0]：このオプションを選択すると、次のフィールドが表示されます。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。
IPv6 スタティックルートの追加	
Prefix	IPv6 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VRF で構成する IPv6 スタティックルートのプレフィックス長を入力します。
Next Hop/Null 0/NAT	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]：ネクストホップ IPv6 アドレスを入力します。 [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Null 0]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv6 Route Null 0]：ネクストホップを null インターフェイスに設定するには、このオプションを有効にします。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [NAT]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv6 NAT]*：NAT64 または NAT66 を選択します。

ACL IPv4

次の表では、ACL IPv4 機能を設定するためのオプションについて説明します。

フィールド	説明
ACL Sequence Name	ACL シーケンスの名前を指定します。
Standard	標準 ACL は、IP パケットの送信元アドレスと ACL に設定されているアドレスを比較して、トラフィックを制御します。
Extended	拡張 ACL は、IP パケットの送信元アドレスおよび宛先アドレスを ACL に設定されているアドレスと比較して、トラフィックを制御します。
Add ACL Sequence	IP パケットに適用される許可および拒否条件を集めたものです。
Import ACL Sequence	デバイスへの ACL シーケンスのインポート。
Drop or Accept	一致が存在するかどうかに応じて実行するアクション。
ACL シーケンスの編集	
ACL Sequence Name	ACL シーケンスの名前を入力します。
Source Address	IP パケットの送信元アドレス
Source Address Host	単一の送信元アドレスホスト
Action Type	デフォルト値は accept です
Accept Actions	標準 IP アクセスリストによって許可または拒否されたパケットに関するメッセージを記録するログをドロップダウンリストから選択します。

[ACL Policy] ウィンドウで特定の ACL シーケンスを選択して、編集、削除、または追加できます。

（注） トランスポートプロファイルおよびサービスプロファイルの設定グループから **ACL ポリシー** 機能を設定することもできます。

管理 VRF

次の表では、管理 VRF 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
Feature Name	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

DNS

フィールド	説明
Add DNS	
Primary DNS Address (IPv4)	この VPN のプライマリ DNS サーバーの IPv4 アドレスを入力します。

ホストマッピング

フィールド	説明
Hostname	DNS サーバーのホスト名を入力します。名前には最大 128 文字を使用できます。
List of IP Address	ホスト名に関連付ける IP アドレスを入力します。エントリをカンマで区切ります。

IPv4/IPv6 スタティックルート

フィールド	説明
IPv4スタティックルートの追加	
Network Address*	IPv4 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VRF で構成する IPv4 スタティックルートのプレフィックス長を入力します。
Subnet Mask*	サブネット マスクを入力します。

フィールド	説明
Gateway*	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [nextHop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv4 アドレスを入力します。 • [Administrative distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • **[dhcp]** • [null0]：このオプションを選択すると、次のフィールドが表示されます。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。
IPv6 スタティックルートの追加	
Prefix*	IPv6 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VRF で構成する IPv6 スタティックルートのプレフィックス長を入力します。
Next Hop/Null 0	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv6 アドレスを入力します。 [Administrative distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Null 0]：このオプションを選択すると、次のフィールドが表示されます。 • [NULL0*]：このオプションを有効にして、ネクストホップを null インターフェイスに設定します。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。

オブジェクトトラッカー

トラッカー機能を使用すると、トラッカーエンドポイントのステータスを追跡できます。

次の表では、オブジェクトトラッカー機能を設定するためのオプションについて説明します。

基本設定

パラメータ名	説明
名前（Name）	トラッカーの名前。名前には128文字以内の英数字を使用できます。最大 8 つのトラッカーを設定できます。
Description	オブジェクトトラッカーの説明を入力します
Object Tracker ID	オブジェクトトラッカーの名前
Interface Name	グローバルまたはデバイス固有のトラッカーインターフェイス名を入力します（例：Gigabitethernet1、Gigabitethernet2）。
Interface Track Type	トランスポート インターフェイスがダウンしていると宣言する前に、プローブが応答を返すのを待機する時間。範囲：100 ～ 1000 ミリ秒。デフォルト：300 ミリ秒。次のオプションがあります。 • Line-protocol • Ip-routing • Ipv6-routing
Route IP	ネットワークのルート IP プレフィックス
Route IP Mask	ネットワークのサブネットマスク
VRF Name	ルート到達可能性を追跡するためのベースとして使用される VRF 名
Delay Up (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストのUPステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。
Delay Down (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストのDownステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。

オブジェクト トラッカー グループ

この機能を使用して、オブジェクト トラッカー グループを設定します。正確なトラッキングのため、オブジェクト トラッカー グループを作成する前に、少なくとも 2 つのオブジェクト トラッカーを追加してください。

基本設定

パラメータ名	説明
Object tracker ID	オブジェクト トラッカー グループの ID を入力します。 範囲：1 ～ 1000
Object tracker	ドロップダウンリストから、以前に作成したオブジェクトトラッカーを 2 つ以上選択します。
Reachable	次の値のいずれかを選択します。 • Either：トラッカーグループの関連付けられたトラッカーのいずれかでルートがアクティブであると報告された場合に、トランスポート インターフェイスのステータスがアクティブと報告されるようにします。 • Both：トラッカーグループの関連付けられたトラッカーの両方でルートがアクティブであると報告された場合に、トランスポート インターフェイスのステータスがアクティブと報告されるようにします。
Delay Up (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの UP ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。
Delay Down (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの Down ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。

ルート ポリシー

特定のパケットを明らかに最短のパス以外の特定のパス経由でルーティングする必要がある場合は、この機能を使用してポリシーベースルーティングを設定します。

次の表では、ルートポリシー機能を設定するためのオプションについて説明します。

フィールド	説明
Routing Sequence Name	ルーティングシーケンスの名前を指定します。
Protocol	インターネットプロトコルを指定します。オプションは、[IPv4]、[IPv6]、またはその両方です。

フィールド	説明
Condition	ルーティング条件を指定します。次のオプションがあります。 • アドレス • AS パスリスト • コミュニティ リスト • 拡張コミュニティリスト • BGP ローカル プリファレンス • Metric • Next Hop • インターフェイス • OSPF タグ
Action Type	アクションタイプを指定します。オプションは、[Accept] または [Reject] です。
Accept Condition	受け入れ条件タイプを指定します。次のオプションがあります。 • AS パス • コミュニティ • ローカルプリファレンス • Metric • Metric Type • Next Hop • 発信元 • OSPF タグ • 重量

VRF

DNS

次の表では、管理 VRF 機能を設定するためのオプションについて説明します。

フィールド	説明
VRF Name	VRF の名前を入力します。
RD	VRF のルート識別子を指定するか、システムデフォルトを使用します。 ルート識別子は、プロバイダーに接続するお客様の個別の仮想プライベート ネットワーク ルートを区別するのに役立ちます。
DNS	
IP Address	この VRF のプライマリ DNS サーバーの IP アドレスを入力します。 この IP アドレスは、Cisco SD-WAN Validator のホスト名を解決するために使用されます。

ホストマッピング

フィールド	説明
新規ホストマッピングの追加	
Hostname	DNS サーバーのホスト名を入力します。最大文字数は 128 文字です。
List of IP	ホスト名に関連付ける IP アドレスを入力します。エントリはカンマで区切ります。

Route

フィールド	説明
IPv4スタティックルートの追加	
Network address	IPv4 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力して、VRF を設定します。
Subnet Mask	プレフィックスやIPアドレスのサブネットマスクを入力します。サブネットマスクはドロップダウンリストからを選択することもできます。

フィールド	説明
Gateway	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add] をクリックすると、次のフィールドが表示されます。 • [Address]：ネクストホップ IPv4 アドレスを指定します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • **オブジェクトトラッカー/オブジェクト トラッカー グループ** オブジェクトトラッキングは、クライアントによって設定された別のオブジェクトでオブジェクトが実行するクライアントアクションをトラッキングするメカニズムです。トラッキング対象の各オブジェクトは、track パラメータで指定される一意の名前で識別できます。 ドロップダウンリストからオブジェクトを選択します。 • [Null 0]：このオプションを有効にすると、ネクストホップが null インターフェイスに設定されます。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • **dhcp** • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Interface]：[Add] をクリックして、次の詳細を指定します。 • [Interface Name]：有効なインターフェイスを指定するか、ドロップダウンリストから値を選択します。 • [Add Next Hop]： • [Address]：ネクストホップ IPv4 アドレスを指定します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。
IPv6 スタティックルート	

フィールド	説明
Prefix	IPv6 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VRF で構成する IPv6 スタティックルートのプレフィックス長を入力します。
Gateway	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add] をクリックすると、次のフィールドが表示されます。 • [Address]：ネクストホップ IPv4 アドレスを指定します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Null 0]：このオプションを有効にすると、ネクストホップが null インターフェイスに設定されます。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Interface]：[Add] をクリックして、次の詳細を指定します。 • [Interface Name]：有効なインターフェイスを指定するか、ドロップダウンリストから値を選択します。 • [Next Hop]： • [Address]：ネクストホップ IPv4 アドレスを指定します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。

NAT

NAT	
NAT Enable	トグルボタンを使用して NAT を有効
Add NAT Interfaces	インターネット側のインターフェイスフェイスを追加します。
Static NAT	静的 NAT マッピングを追加します。
Static NAT Subnet	NAT マッピングのサブネットを定義

NAT Port Forward	NAT ポート フォワーディング ル
Dynamic NAT	ダイナミック NAT ルールを定義し

ルートリーク

グローバル VRF からのルートリーク	
Route Protocol	表示されるオプションから、グローバル VRF から設定中のサービス VRF にルートをリークするプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。
再配布（VRF）	
Protocol	表示されるオプションから、リークされたルートを再配布するプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。
グローバル VRF へのルートリーク	
Route Protocol	表示されるオプションから、設定中のサービス VRF からグローバル VRF にルートをリークするプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。
再配布（グローバル VRF）	
Protocol	表示されるオプションから、リークされたルートを再配布するプロトコルを選択します。
Select Route Policy	ルートポリシーの名前を入力します。
他のサービス VRF からのルートリーク	
Source VRF	送信元 VRF の値を入力します。
Route Protocol	表示されるオプションから、送信元のサービス VRF から設定中のサービス VRF にルートをリークするプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。
再頒布（サービス VRF）	
Protocol	表示されるオプションから、リークされたルートを再配布するプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。

イーサネット インターフェイス

この機能は、VPN でイーサネット インターフェイスを設定するのに役立ちます。

次の表では、イーサネットインターフェイス機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから VRF を選択します。
Associated VRF	VRF を選択します。

基本設定

フィールド	説明
Shutdown	インターフェイスを有効または無効にします。
Control Connection	トンネルで制御接続を有効にするには、[on] を選択します。
Bind Interface	ループバックインターフェイスにバインドする物理インターフェイスの名前を入力します。
Interface Name	インターフェイスの名前を入力します。インターフェイス名を完全にスペルアウトします (たとえば、GigabitEthernet0/0/0)。 使用していない場合でも、ルータのすべてのインターフェイスを構成して、それらがシャットダウン状態で構成され、それらのすべてのデフォルト値が構成されるようにします。
Description	インターフェイスの説明を入力します。
IPv4 Settings	IPv4 VRF インターフェイスを設定します。 • [Dynamic]：インターフェイスを Dynamic Host Configuration Protocol（DHCP）クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。 • [Static]：変更されない IP アドレスを入力するには、[Static] を選択します。
Dynamic DHCP Distance	DHCP サーバーから学習したルートのアドミニストレーティブディスタンス値を入力します。このオプションは、[Dynamic] を選択した場合に使用できます。 デフォルト：1
IPv4 Settings	静的 IPv4 アドレスを入力します。このオプションは、[Static] を選択した場合に使用できます。 の「Configuring RAID Levels」の章を参照してください。
Subnet Mask	サブネットマスクを入力します。

フィールド	説明
Configure Secondary IP Address	サービス側インターフェイスのセカンダリ IPv4 アドレスを最大 4 つ入力します。 • [IP Address]：IP アドレスを入力します。 • [Subnet Mask]：サブネットマスクを入力します。
DHCP Helper	インターフェイスをルータの DHCP ヘルパーとして指定するには、ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力します。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。
IPv6 Settings	IPv6 VPN インターフェイスを設定します。 • [Dynamic]：インターフェイスを Dynamic Host Configuration Protocol（DHCP）クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。 • [Static]：変更されない IP アドレスを入力するには、[Static] を選択します。 • **None**
IPv6 Address Primary	静的 IPv6 アドレスを入力します。このオプションは、[Static] を選択した場合に使用できます。

BFD

フィールド	説明
Enable BFD	リンク障害を検出するには、このオプションを有効にします

ARP

フィールド	説明
IP Address	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
MAC Address	MAC アドレスをコロン区切りの 16 進表記で入力します。

ACL

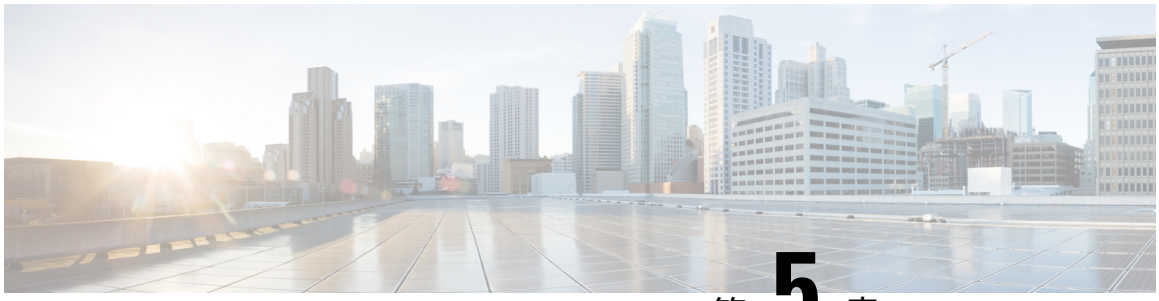
フィールド	説明
ACL IPv4 Ingress	インターフェイスで受信されるパケットに対して使用する IPv4 アクセスリストの名前を指定します。
ACL IPv4 Egress	インターフェイスから送信されるパケットに対して使用する IPv4 アクセスリストの名前を指定します。
ACL IPv6 Ingress	インターフェイスで受信されるパケットに対して使用する IPv6 アクセスリストの名前を指定します。
ACL IPv6 Egress	インターフェイスから送信されるパケットに対して使用する IPv6 アクセスリストの名前を指定します。

Advanced

フィールド	説明
Duplex	インターフェイスが全二重または半二重のどちらのモードで実行されるかを指定します。 デフォルト：full
MAC Address	インターフェイスに関連付ける MAC アドレスを、コロンで区切った 16 進表記で指定します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：576 ～ 9216 デフォルト：1500 バイト
Interface MTU	インターフェイスで送受信されるフレームの最大伝送単位サイズを入力します。 範囲：1500 ～ 1518（GigabitEthernet0）、1500 ～ 9216（他の GigabitEthernet） デフォルト：1500 バイト
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：500 ～ 1460 バイト デフォルト：なし

フィールド	説明
Speed	接続のリモートエンドが自動ネゴシエーションをサポートしていない場合に使用する、インターフェイスの速度を指定します。 値：10、100、1000、2500、または 10000 Mbps
ARP Timeout	ARP タイムアウトは、ルータで ARP キャッシュを保持する期間を制御します。動的に学習された ARP エントリがタイムアウトするまでの時間を指定します。 範囲：0 ～ 2147483 秒 デフォルト：1200 秒
Autonegotiate	自動ネゴシエーションをオンにするには、このオプションを有効にします。
Media Type	インターフェイスの物理メディア接続タイプを指定します。次のいずれかを選択します。 • [auto-select]：接続は自動的に選択されます。 • [rj45]：RJ-45 の物理接続を指定します。 • [sfp]：光ファイバメディアの Small Form Factor Pluggable（SFP）物理接続を指定します。
Load Interval	インターフェイス負荷計算の間隔値を入力します。

フィールド	説明
IP Directed Broadcast	IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。 宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクト ブロードキャストを転送します。ダイレクト ブロードキャスト パケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。 あるインターフェイスでダイレクト ブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクト ブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。
ICMP Redirect Disable	ICMP リダイレクトは、パケットが最適にルーティングされていないときに、ルータによって IP パケットの送信者に送信されます。ICMP リダイレクトは、送信側ホストに対し、後続のパケットを別のゲートウェイ経由で同じ宛先に転送するように通知します。 デフォルトでは、インターフェイスは ICMP リダイレクトメッセージを許可します。



第 5 章

サービス プロファイル

ACL IPv4

次の表では、ACL IPv4 機能を設定するためのオプションについて説明します。

フィールド	説明
ACL Sequence Name	ACL シーケンスの名前を指定します。
Standard	標準 ACL は、IP パケットの送信元アドレスと ACL に設定されているアドレスを比較して、トラフィックを制御します。
Extended	拡張 ACL は、IP パケットの送信元アドレスおよび宛先アドレスを ACL に設定されているアドレスと比較して、トラフィックを制御します。
Add ACL Sequence	IP パケットに適用される許可および拒否条件を集めたものです。
Import ACL Sequence	デバイスへの ACL シーケンスのインポート。
Drop or Accept	一致が存在するかどうかに応じて実行するアクション。
ACL シーケンスの編集	
ACL Sequence Name	ACL シーケンスの名前を入力します。
Source Address	IP パケットの送信元アドレス

フィールド	説明
Source Address Host	単一の送信元アドレスホスト
Action Type	デフォルト値は accept です
Accept Actions	標準 IP アクセスリストによって許可または拒否されたパケットに関するメッセージを記録するログをドロップダウンリストから選択します。

[ACL Policy] ウィンドウで特定の ACL シーケンスを選択して、編集、削除、または追加できます。

（注） トランスポートプロファイルおよびサービスプロファイルの設定グループから **ACL ポリシー** 機能を設定することもできます。

DHCP サーバ

この機能を使用すると、インターフェイスを DHCP ヘルパーとして設定して、DHCP サーバーから受信したブロードキャスト DHCP 要求を転送することができます。

この機能のデフォルト値を持つ各パラメータでは、範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンをクリックし、次のいずれかを選択します。

基本設定

フィールド	説明
Address Pool	ルータインターフェイスが DHCP サーバーとして機能するサービス側ネットワークのアドレスプールの IPv4 プレフィックス範囲を、**`prefix/length`** の形式で入力します。
Exclude	DHCP アドレスプールから除外する 1 つ以上の IP アドレスを入力します。複数の個別のアドレスを指定するには、それらをカンマで区切ってリストします。アドレスの範囲を指定するには、ハイフンで区切ります。
Lease Time(seconds)	DHCP によって割り当てられた IP アドレスが有効である時間を指定します 範囲：60 ～ 31536000 秒 デフォルト：86400

静的リース

フィールド	説明
Add Static Lease	
MAC Address	静的 IP アドレスが割り当てられるクライアントの MAC アドレスを入力します。
IP	クライアントに割り当てる静的 IP アドレスを入力します。

DHCP オプション

フィールド	説明
Add Option Code	
Code	オプションコードを設定します。 範囲：1 ～ 254
Type	次の 3 つのタイプのいずれかを選択します。 • [ASCII]：ASCII 値を指定します。 • [Hex]：16 進値を指定します。 • [IP]：IP アドレスを指定します。最大 8 つの IP アドレスを指定できます。

Advanced

フィールド	説明
Interface MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：68 ～ 65535 バイト
Domain Name	DHCP クライアントがホスト名を解決するために使用するドメイン名を指定します。
Default Gateway	サービス側ネットワークのデフォルトゲートウェイの IP アドレスを入力します。
DNS Servers	サービス側ネットワークの DNS サーバーの IP アドレスを 1 つ以上入力します。複数のエントリがある場合は、カンマで区切ります。最大 8 つのアドレスを指定できます。

フィールド	説明
TFTP Servers	サービス側ネットワークの TFTP サーバーの IP アドレスを入力します。1 つまたは 2 つのアドレスを指定できます。2 つの場合、アドレスはカンマで区切ってください

オブジェクトトラッカー

トラッカー機能を使用すると、トラッカーエンドポイントのステータスを追跡できます。

次の表では、オブジェクトトラッカー機能を設定するためのオプションについて説明します。

基本設定

パラメータ名	説明
名前（Name）	トラッカーの名前。名前には128文字以内の英数字を使用できます。最大 8 つのトラッカーを設定できます。
Description	オブジェクトトラッカーの説明を入力します
Object Tracker ID	オブジェクトトラッカーの名前
Interface Name	グローバルまたはデバイス固有のトラッカーインターフェイス名を入力します（例：Gigabitethernet1、Gigabitethernet2）。
Interface Track Type	トランスポート インターフェイスがダウンしていると宣言する前に、プローブが応答を返すのを待機する時間。範囲：100 ～ 1000 ミリ秒。デフォルト：300 ミリ秒。次のオプションがあります。 • Line-protocol • Ip-routing • Ipv6-routing
Route IP	ネットワークのルート IP プレフィックス
Route IP Mask	ネットワークのサブネットマスク
VRF Name	ルート到達可能性を追跡するためのベースとして使用される VRF 名
Delay Up (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの UP ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。
Delay Down (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの Down ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。

オブジェクト トラッカー グループ

この機能を使用して、オブジェクト トラッカー グループを設定します。正確なトラッキングのため、オブジェクト トラッカー グループを作成する前に、少なくとも 2 つのオブジェクト トラッカーを追加してください。

基本設定

パラメータ名	説明
Object tracker ID	オブジェクト トラッカー グループの ID を入力します。 範囲：1 ～ 1000
Object tracker	ドロップダウンリストから、以前に作成したオブジェクトトラッカーを 2 つ以上選択します。
Reachable	次の値のいずれかを選択します。 • Either：トラッカーグループの関連付けられたトラッカーのいずれかでルートがアクティブであると報告された場合に、トランスポート インターフェイスのステータスがアクティブと報告されるようにします。 • Both：トラッカーグループの関連付けられたトラッカーの両方でルートがアクティブであると報告された場合に、トランスポート インターフェイスのステータスがアクティブと報告されるようにします。
Delay Up (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの UP ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。
Delay Down (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの Down ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。

ルート ポリシー

特定のパケットを明らかに最短のパス以外の特定のパス経由でルーティングする必要がある場合は、この機能を使用してポリシーベースルーティングを設定します。

次の表では、ルートポリシー機能を設定するためのオプションについて説明します。

フィールド	説明
Routing Sequence Name	ルーティングシーケンスの名前を指定します。

フィールド	説明
Protocol	インターネットプロトコルを指定します。オプションは、[IPv4]、[IPv6]、またはその両方です。
Condition	ルーティング条件を指定します。次のオプションがあります。 • アドレス • AS パスリスト • コミュニティ リスト • 拡張コミュニティリスト • BGP ローカル プリファレンス • Metric • Next Hop • インターフェイス • OSPF タグ
Action Type	アクションタイプを指定します。オプションは、[Accept] または [Reject] です。
Accept Condition	受け入れ条件タイプを指定します。次のオプションがあります。 • AS パス • コミュニティ • ローカルプリファレンス • Metric • Metric Type • Next Hop • 発信元 • OSPF タグ • 重量

VRF

DNS

次の表では、管理 VRF 機能を設定するためのオプションについて説明します。

フィールド	説明
VRF Name	VRF の名前を入力します。
RD	VRF のルート識別子を指定するか、システムデフォルトを使用します。 ルート識別子は、プロバイダーに接続するお客様の個別の仮想プライベート ネットワーク ルートを区別するのに役立ちます。
DNS	
IP Address	この VRF のプライマリ DNS サーバーの IP アドレスを入力します。 この IP アドレスは、Cisco SD-WAN Validator のホスト名を解決するために使用されます。

ホストマッピング

フィールド	説明
新規ホストマッピングの追加	
Hostname	DNS サーバーのホスト名を入力します。最大文字数は 128 文字です。
List of IP	ホスト名に関連付ける IP アドレスを入力します。エントリはカンマで区切ります。

Route

フィールド	説明
IPv4スタティックルートの追加	
Network address	IPv4 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力して、VRF を設定します。
Subnet Mask	プレフィックスやIPアドレスのサブネットマスクを入力します。サブネットマスクはドロップダウンリストからを選択することもできます。

フィールド	説明
Gateway	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add] をクリックすると、次のフィールドが表示されます。 • [Address]：ネクストホップ IPv4 アドレスを指定します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • **オブジェクトトラッカー/オブジェクト トラッカー グループ** オブジェクトトラッキングは、クライアントによって設定された別のオブジェクトでオブジェクトが実行するクライアントアクションをトラッキングするメカニズムです。トラッキング対象の各オブジェクトは、track パラメータで指定される一意の名前で識別できます。 ドロップダウンリストからオブジェクトを選択します。 • [Null 0]：このオプションを有効にすると、ネクストホップが null インターフェイスに設定されます。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • **dhcp** • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Interface]：[Add] をクリックして、次の詳細を指定します。 • [Interface Name]：有効なインターフェイスを指定するか、ドロップダウンリストから値を選択します。 • [Add Next Hop]： • [Address]：ネクストホップ IPv4 アドレスを指定します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。
IPv6 スタティックルート	

フィールド	説明
Prefix	IPv6 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VRF で構成する IPv6 スタティックルートのプレフィックス長を入力します。
Gateway	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add] をクリックすると、次のフィールドが表示されます。 • [Address]：ネクストホップ IPv4 アドレスを指定します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Null 0]：このオプションを有効にすると、ネクストホップが null インターフェイスに設定されます。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Interface]：[Add] をクリックして、次の詳細を指定します。 • [Interface Name]：有効なインターフェイスを指定するか、ドロップダウンリストから値を選択します。 • [Next Hop]： • [Address]：ネクストホップ IPv4 アドレスを指定します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。

NAT

NAT	
NAT Enable	トグルボタンを使用して NAT を有
Add NAT Interfaces	インターネット側のインターフェイスを追加します。
Static NAT	静的 NAT マッピングを追加します
Static NAT Subnet	NAT マッピングのサブネットを定

NAT Port Forward	NAT ポート フォワーディング ルール
Dynamic NAT	ダイナミック NAT ルールを定義しま

ルートリーク

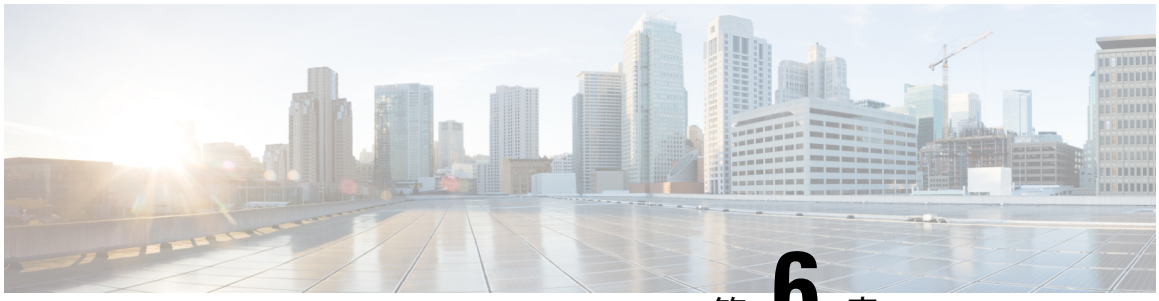
グローバル VRF からのルートリーク	
Route Protocol	表示されるオプションから、グローバル VRF から設定中のサービス VRF にルートをリークするプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。
再配布（VRF）	
Protocol	表示されるオプションから、リークされたルートを再配布するプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。
グローバル VRF へのルートリーク	
Route Protocol	表示されるオプションから、設定中のサービス VRF からグローバル VRF にルートをリークするプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。
再配布（グローバル VRF）	
Protocol	表示されるオプションから、リークされたルートを再配布するプロトコルを選択します。
Select Route Policy	ルートポリシーの名前を入力します。
他のサービス VRF からのルートリーク	
Source VRF	送信元 VRF の値を入力します。
Route Protocol	表示されるオプションから、送信元のサービス VRF から設定中のサービス VRF にルートをリークするプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。
再頒布（サービス VRF）	
Protocol	表示されるオプションから、リークされたルートを再配布するプロトコルを選択します。
Select Route Policy	ドロップダウンリストからルートポリシーを選択します。

IPv4/IPv6スタティックルートサービス

IPv4/IPv6 スタティックルート

フィールド	説明
IPv4スタティックルートの追加	
IP Address*	IPv4 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VPN で構成する IPv4 スタティック ルートのプレフィックス長を入力します。
Subnet Mask*	サブネット マスクを入力します。
Gateway*	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [nextHop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv4 アドレスを入力します。 • [Administrative distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • **[dhcp]** • [null0]：このオプションを選択すると、次のフィールドが表示されます。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。
IPv6 スタティックルートの追加	
Prefix*	IPv6 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VPN で構成する IPv6 スタティック ルートのプレフィックス長を入力します。

フィールド	説明
Next Hop/Null 0/NAT	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv6 アドレスを入力します。 [Administrative distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Null 0]：このオプションを選択すると、次のフィールドが表示されます。 • [NULL0*]：このオプションを有効にして、ネクストホップを null インターフェイスに設定します。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [NAT]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv6 NAT]：NAT64 または NAT66 を選択します。



第 6 章

ポリシー オブジェクト プロファイル

ポリシーオブジェクト機能プロファイルを使用すると、ポリシー構成をデバイスにアタッチできます。

次の表に、ポリシープロファイルを構成するためのオプションを示します。

表 *4:*

フィールド	説明
Choose existing	[Profiles] テーブルから既存のプロファイルを選択します。
Create new	このオプションを選択すると、次のフィールドが表示されます。 • [Name]：プロファイルの名前を入力します。 • [Description]：プロファイルの説明を入力します。説明では、 文字とスペースを使用できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。